Institutional Foundations for Cyber Security: Current Responses and New Challenges

Jeremy Ferwerda
Nazli Choucri
Stuart Madnick

Working Paper CISL# 2009-03

September 2010

Composite Information Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Institutional Foundations for Cyber Security: Current Responses and New Challenges	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Massachusetts Institute of Technology,Composite Information Systems Laboratory (CISL),Sloan School of Management, Room E62-422,Cambridge,MA,02142**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This paper profiles institutions that are responsible for addressing threats to cyber security. Rather than focusing primarily on the private sector, we analyze key organizations at the national, international, and intergovernmental level. Our purpose is to highlight emerging responses and challenges, while simultaneously evaluating the strengths and weaknesses of the current institutional framework. A secondary goal is to investigate the feasibility of using quantitative data to evaluate cyber security performance.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**28**	

Institutional Foundations for Cyber Security: Current Responses and New Challenges

Jeremy Ferwerda
Nazli Choucri
Stuart Madnick
Massachusetts Institute of Technology

Abstract

This paper profiles institutions that are responsible for addressing threats to cyber security. Rather than focusing primarily on the private sector, we analyze key organizations at the national, international, and intergovernmental level. Our purpose is to highlight emerging responses and challenges, while simultaneously evaluating the strengths and weaknesses of the current institutional framework. A secondary goal is to investigate the feasibility of using quantitative data to evaluate cyber security performance.

Keywords: cyber security, cyber governance, cyber institutions, international security

I. Introduction

The expansion of cyberspace has occurred at a dramatic pace over the past two decades. Almost every location in the globe now has some degree of cyber access, outpacing even the most optimistic expectations of the early architects of the Internet. Less anticipated, however, by the initial innovators or anyone else, was the subsequent introduction of cyber threats and the accompanying innovations in the disruption and distortion of cyber venues. This evolution of security concerns has created two broad sets of uncertainties. First, there are ambiguities and challenges surrounding the empirical assessment of threats, actions, and events. Second, and more critically, there is a marked absence of integrated global institutional mechanisms designed to track, record and respond to cyber incidents.

The purpose of this paper is to take stock of current institutional responses to cyber threats at the international level and to the extent possible, at the national level as well. Our goal is to 'base-line' the emergence of organizational responses to a rapidly changing cyber security landscape. We ask: who are the major actors? What are their missions and responsibilities? Can we begin to discern the emergence of a fabric of global governance for cyberspace?

Framing the Context

Throughout the early years of Internet development, security was not established or maintained via a formal or planned institutional framework. Instead, the critical roles of threat detection and mitigation were largely left to the private sector. Companies were expected to handle security for their own products, and users accepted some inherent risk or liability. However, this approach was never suited to handle significant growth in vulnerabilities. Individual corporations lacked incentives to share information, and more importantly, lacked the legal authority to deal with emerging national threats or to prosecute criminal networks. As a result, response to cyber incidents remained closeted and uncoordinated, with private entities adopting a largely reactive approach.

Observing this situation, several non-profit organizations attempted to fill the organizational gap by providing volunteer response teams, information sharing networks, and security guidelines. By focusing on issues that spanned the corporate barrier, these non-profit organizations established a foundation for coordinated community response to emerging cyber threats. However, although they were often successful at mitigating localized security issues, non-profit organizations lacked the requisite authority and resources to effectively respond to crises of global or national scope.

Over the better part of a decade, the convergence of four distinct but interconnected trends created demands for formal interventions involving governments and international coordination. First, internet usage continued to rise, coupled with an expansion in forms of use. Second, many governments recognized that cyber vulnerabilities continued to threaten not only the security of their own networks but also those of their citizens involved in routine activities on a daily basis.

Third, there was a noted absence of coordinated industry responses or of efforts to develop cooperative threat reduction strategies, thereby reinforcing an unambiguous gap-in-governance. Finally, a growing set of cyber incidents, large and small, signaled to governments the potential impact of their failure to address the emerging threat. In response, governments, in various ways, mobilized significant national and international resources towards the creation of a broad cyber security framework; the resulting institutional responses serve as the focus of this paper.

The Institutional 'Eco-System'

By way of orientation, Table 1 identifies the organizations and entities referred to in this paper. A cursory look at this table indicates that the cyber security 'institutional eco-system' is a complex assortment of national, international, and private organizations. Parallel to the organic fashion in which cyberspace itself developed, these organizations often have unclear mandates or possess overlapping spheres of influence. At this stage we seek only to highlight the major entities and, to the extent possible, to signal their relationships and interconnections. A secondary, but also important, objective is to explore data quality and the extent to which we may infer organizational performance from public metrics.

Throughout this analysis, we will refer to two separate categories of malfeasance: *cyber threats* and *cyber crime*. The former involves the exploitation of infrastructural weaknesses and security vulnerabilities. Responses to these threats often involve technical rather than legal measures; as such, a variety of organizations ranging from non-profit entities to intergovernmental bodies are actively involved in defense. In contrast, cyber crime refers exclusively to attacks on private entities with the intent of gaining profit or inflicting damage. Although cyber crime can be mitigated by enhancing the security of internet networks, only national governments possess the proper legal tools and jurisdiction to prosecute attackers. As a result, effective response to cyber crime is largely restricted to sovereign entities.

It should be noted that although this paper catalogues many of the major institutional players, it is not exhaustive. Two criteria were used to select organizations for analysis. First, we focused on entities that provide public qualitative or quantitative data. Second, within each of our three areas of focus (International, Intergovernmental, and National) we selected institutions with coordinating responsibility or formal mandates issued by recognized international or national bodies. For the national sphere, we focused on the United States as a representative model; detailed analysis of other national efforts is beyond the scope of this paper.

Table 1. International Institutional Eco-System

Institution	Role	Data Availability	Example Variables (where applicable)
CERTs			
AP-CERT: Asia Pacific Computer Emergency Response Team	Asian regional coordination	High	Collation of security metrics from member CERTs in Asia.
CERT-CC: Computer Emergency Response Team - Coordination Center	Coordination of global CERTs, especially national CERTs.	Moderate	Vulnerabilities catalogued, Hotline calls received, Advisories & alerts published, Incidents handled
FIRST: Forum for Incident Response and Security Teams	Forum and information sharing for CERTs	Low	Secondary data from conferences and presented papers
National CERTs	National coordination; national defense & response	High	Varies - Volume of malicious code & viruses, Vulnerability alerts, Botnets, Incident reports
TF-CSIRT: Collaboration of Security Incident Response Teams	European regional coordination	N/A	N/A
International Entities			
CCDCOE: Cooperative Cyber Defence Centre of Excellence	Enhancing NATO's cyber defense capability	N/A*	N/A*
Council of Europe	International Legislation	Moderate	Legislation & ratification statistics; Secondary data from conferences and presented papers.
European Union	Sponsors working parties, action plans, guidelines	N/A	N/A
ENISA: European Network and Information Security Agency	Awareness raising, cooperation between the public and private sectors, advising the EU on cyber security issues, data collection	Low	Awareness raising stats, spam surveys, Regional surveys, Country reports. Qualitative data assessing the EU cyber security sphere.
G8: Subgroup on High Tech Crime	Sponsored 24/7 INTERPOL hotline, various policy guidelines	N/A	N/A
IMPACT: International Multilateral Partnership Against Cyber Threats	Global threat response center, data analysis, real-time early warning system	N/A*	N/A*
INTERPOL: International Criminal Police Organization	Manages 24/7 hotline, trains law enforcement agencies, participates in investigations.	N/A	N/A
ITU: International Telecommunications Union	Sponsors IMPACT. Organizes conferences, releases guidelines and toolkits, facilitates information exchange and cooperation.	Moderate	Internet usage and penetration statistics; Secondary data from conferences & presented papers

NATO: North Atlantic Treaty Organization	Responding to military attacks on NATO member states	N/A	N/A: Classified
OECD: Organisation for Economic Co-operation and Development	Develops policy options, organizes conferences, publishes guidelines and best-practices.	Low	Secondary data from conferences and presented papers
UNODC: United Nations Office on Drugs & Crime	Promotion of legislation, training programs, awareness, enforcement	N/A	N/A
WSIS: World Summit on the Information Society	Global summit on information security; publishes resolutions and monitors implementation through stocktaking efforts.	Low	Stocktaking database & Secondary data from conferences and presented papers
National Entities			
CIA: Central Intelligence Agency	Defense of intelligence networks, information gathering.	N/A	N/A: Classified
DHS: Department of Homeland Security	Protection of federal civil networks & critical infrastructure; information sharing and awareness; coordinating federal response and alerts.	N/A	N/A: Unclassified data released through US-CERT
DoD: Department of Defense	Defense of military networks, counterattack capability.	N/A	N/A: Classified
DOJ: US Department of Justice	Federal Prosecution	Moderate	Non aggregated data: Prosecuted Cases, Crime by industry
FBI: Federal Bureau of Investigation	Federal Investigation	Low	Total reported incidents, Number of referrals to law enforcement agencies. Annual surveys on corporate computer crime including: Type and frequency of attacks, Dollar loss, Attack source
FTC: Federal Trade Commission	Consumer Protection	N/A	N/A
IC3: Internet Crime Complaint Center	Cybercrime Reporting & Referral Center	High	Total complaints, Referred complaints, Estimated dollar loss, Complaints by industrial sector
NW3C: National White Collar Crime Center	Provides training and support to law enforcement agencies, helps administer the IC3 with the FBI.	N/A	N/A: statistics released through IC3
Secret Service	Investigation of economic cyber crimes.	N/A	N/A
US-CERT: United States Computer Emergency Response Team	Defense of federal civil networks (.gov), information sharing and collaboration with private sector.	Moderate	Incidents and events by category, Vulnerability reports
National Police Bureaus (For example: Taiwan, South Korea, Japan, United States, France, Germany, UK)	Investigation, Enforcement	Varies	Cases, Arrests, Prosecutions, Demographics

II. International Institutional Response

First, we consider two sets of institutions that are international but not intergovernmental in scope. We begin with a brief overview of *Computer Emergency Response Teams* (CERTS)[1], and then examine a subset of collaborative organizations that coordinate CERT policy.

CERTS

An important addition to the dense network of international entities in the 'real' arena, CERTs occupy a salient role in the internet security landscape. As defined by the CERT Coordination Center (CERT/CC), these teams organize responses to security emergencies, promote the use of valid security technology, and ensure network continuity (CERT Program, 2009a). In principle, this means that CERTs focus on identifying vulnerabilities and fostering communication between security vendors, users, and private organizations. Although the majority of CERTs were founded as non-profit organizations, many have transitioned towards public-private partnerships in recent years. This increasing level of integration with national governments represents an attempt to build upon the successes of non-profit CERTs by providing a level of structure and resources hitherto unavailable. However, it is important to note that while the CERT network is becoming increasingly organized, individual CERTs may differ considerably in their ability to effectively perform their mandates. At present, there are over 200 recognized CERTs, with widely different levels of organization, funding, and expertise (Forum of Incident Response and Security Teams, 2009a).

At least three products are expected to result from CERT activities and interactions: a reduction in unaddressed security vulnerabilities, improved understanding of the nature and frequency of cyber threats, and improved methods of communicating and reporting these threats to other security teams and the general public. From a data perspective, it is important to recognize that although CERTS are not established to serve as information gathering institutions *per se,* their activities involve active threat monitoring and information exchange. As a result, many CERTs attempt to provide quantitative data for the cyber security community. It should be noted, however, that there is currently little effort to align or coordinate methods of data collection, and availability and reliability of reported information thus varies widely across the CERT landscape (Madnick et al, 2009).

Organizational Structure

In general, CERTs share a common structure and backbone. The majority of CERT teams are defined according to guidelines originally published by CERT/CC, and many use common toolkits to establish their organizations (Killcrece, 2004). As a result, CERTs tend to differ from

[1] These organizations are also referred to as Computer Security Incident Response Teams (CSIRTs).

each other mainly in their area of focus (academic, private, national, regional), or their respective area of expertise (phishing, viruses, information security). These roles are largely self-defined according to each team's level of funding (which can vary widely), technical expertise, and the presence of perceived gaps within the CERT collaborative network. One expected advantage of this underlying flexibility is that it greatly improves the possibility of coordination between CERTs. However, this loose network also reduces the locus of responsibility or accountability for individual performance. To illustrate the complexity of arrangements, Figure 1 presents a subset of these structured relationships at different levels of analysis of organization.

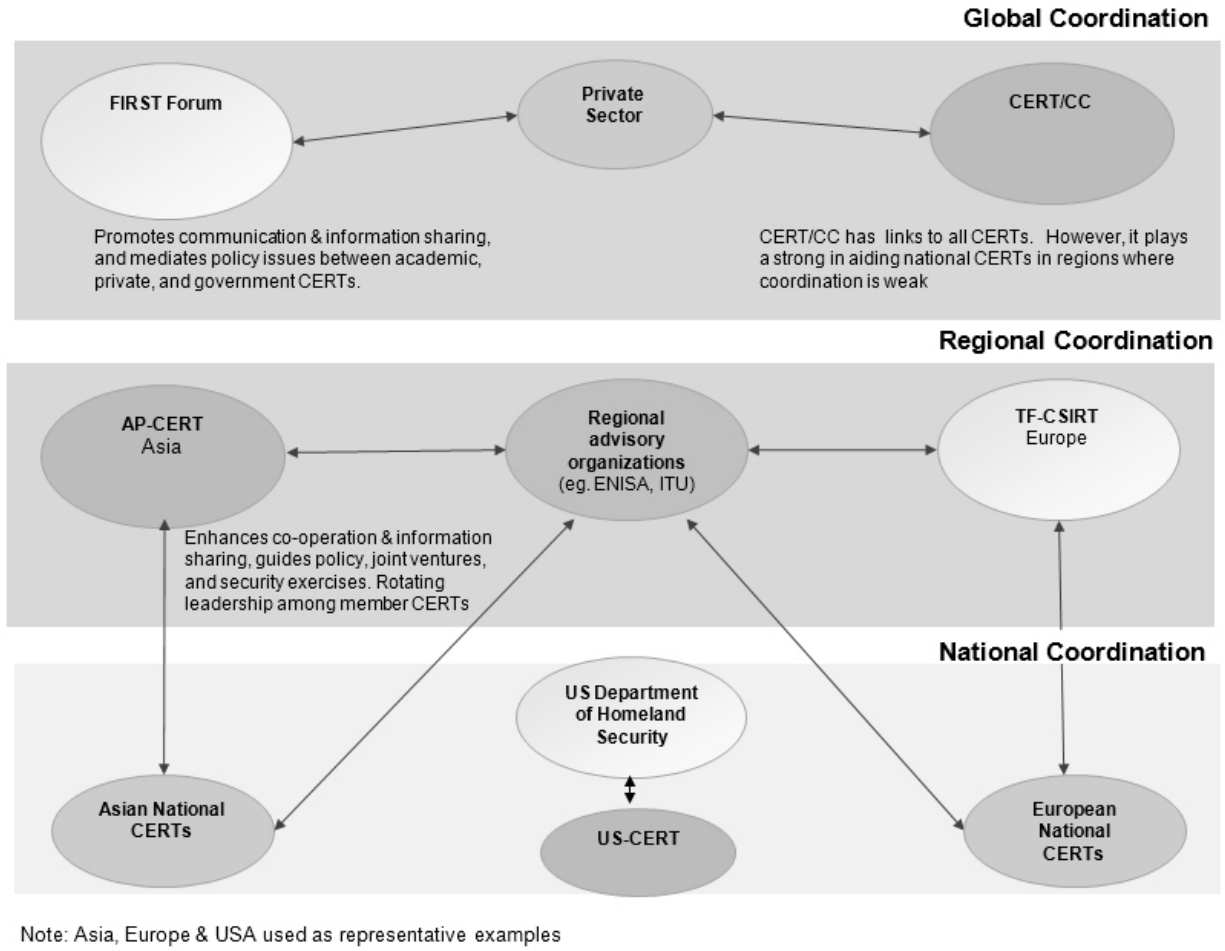


Figure 1. International CERTs

Coordinating Organizations

A distinguishing feature of the CERT system is its coordinating mechanism. Established at Carnegie Mellon University in 1998 in response to a major internet worm, CERT/CC was the first operational CERT, and defined many of the parameters of the role. The Defense Advanced Research Projects Agency (DARPA) originally provided federal funding for the organization with the assumption that CERT/CC would serve as a center for direct threat assessment and response. However, as cyberspace expanded, a single organization proved insufficient to handle the increasing volume of security incidents, and CERT/CC was forced to reframe its activities and priorities. Rather than responding directly to emerging incidents, CERT/CC chose to utilize the lessons it had learned to provide guidelines, coordination, and standards for other CERTs. By relinquishing operational control in favor of a collaborative structure, CERT/CC laid the foundation for the establishment of regional, focused organizations. Today, the CERT network has expanded beyond the scope and control of CERT/CC, although the organization continues to play an influential role in establishing national CERTs in developing countries and fostering CERT communication.

In addition to CERT/CC, many CERTS also interact with parallel coordination networks, such as the *Forum of Incident Response and Security Teams* (FIRST). This body was established to enhance information sharing between disparate security groups (FIRST, 2009b). Now composed of more than 200 organizations, FIRST is notable for its influential annual conferences and its extensive integration of national, academic, and private CERT teams (FIRST, 2009a).

National CERTs

The collaborative structure maintained by coordinating agencies such as FIRST and CERT/CC clearly aids in enhancing information flow between security teams. However, if CERTs were only organized in this fashion, it would be unclear which organizations possessed regional authority to coordinate the actions of other CERTs; for instance, in the event of a national attack on civilian networks. This problem was addressed by transitioning the CERT structure to a national level. One valuable side effect of this shift to national-level jurisdiction was the creation of public-private partnerships between national CERTs and national agencies.

However, a solution to one problem can often give rise to additional complications. Given the diversity of national political systems and bureaucratic practices, the transition to national CERTs exacerbated the realities of legal and jurisdictional diversity. For example, while some national CERTs, such as US-CERT, were specifically tasked by the federal government to defend civilian networks, other organizations operate in a legal vacuum, and assume national responsibility via general consensus. Often, this legitimacy is granted by regional organizations such as AP-CERT in Asia and TF-CERT in Europe that steer regional CERT policy. While this diversity is not

necessarily a problem, it may impede information sharing, and suggests that national CERTs may or may not be held to international operating standards.

It is important to recognize that although national CERTs are endowed with regional authority, they remain restricted in their capacity to respond to cyber criminals. National CERTs occupy a first-line responder role in the event of attacks on national civilian networks, but lack the jurisdictional authority to shut down criminal networks and prosecute perpetrators. As a result, national CERTs focus primarily on responding to and preventing *technical* cyber threats. In order to effectively deal with legal issues, clear lines of communication between national CERTs and government agencies are essential. Although this link has been formalized in some countries such as the United States, other nations are still developing the requisite connections between national CERTs and legal authority.

CERT Data Provision

It is unfortunate that the high level of CERT cooperation and standardization does not extend to the collection of quantitative data. As suggested earlier, data availability varies widely between CERTs, and organizations that publish statistics do not necessarily use similar reporting methods. Moreover, there are no efforts underway to formally align and standardize metrics. In general, the lack of robust data can be traced to three underlying factors. First, it is inherently difficult to quantify cyber data due to uncertainties surrounding the nature, geographical location, and target of attacks. The rapid pace of technological development, coupled with a lack of standards-providing organizations has thus led to significant disparities in the diagnosis and classification of cyber events. Second, many CERTs lack a compelling business reason to gather or verify the accuracy of their quantitative data. CERTs typically possess limited funding capacity and many organizations choose to allocate their resources to cyber response in lieu of robust data collection. Lastly, there is no central authority or volunteer organization tasked with disseminating, collecting, or verifying CERT data.

Although quantitative data is fragmented, the collaborative nature of the CERT network means that a significant amount of information remains available on CERT activities. From a research standpoint, CERT/CC and FIRST provide a means to analyze global CERT policy. In addition, CERT/CC provides a variety of data sources that can be used to evaluate historical CERT activity. These statistics include the number of security alerts, vulnerability notes, and advisories published per year. Although these figures are self-reported and the threshold necessary to publish an alert may vary from year to year, they provide a baseline for estimating global CERT activity. This analysis can be complemented by CERT/CC statistics on the number of incident reports and hotline calls received from member organizations and national CERTs.[2]

[2] Unfortunately, CERT/CC has announced that no statistics will be published after Q3 2008. As a result, analysis is limited to historical applications (1988-2008).

Useful information can also be gleaned by viewing aggregate data at the regional level. In particular, AP-CERT and several other regional bodies publish statistics that cover the number of incidents handled and reported, attack vectors, counts of defaced websites, and other Web vulnerabilities. While these statistics are not as robust as those provided by the private sector, they are partitioned along national lines and provide country-specific statistics that are valuable for analyzing divergent responses to cyber threats. By coupling this information with widely available metrics such as internet connectivity or arrest rates, and controlling for data quality, it may be possible to develop a statistical model to analyze the overall effectiveness of cyber defense across nations.

III. Inter-Governmental Organizations

Although CERTs occupy an important role in the international security ecosystem, their core competencies or self-defined responsibilities do not extend to consensus building, legislation, or awareness-raising. While this set of functions remained largely unclaimed in the nascent years of internet development, they have recently been embraced by a variety of intergovernmental organizations.

By definition international organizations consist of sovereign states. All of the major international organizations and many minor ones were established long before the creation of cyberspace. They are major users of cyber venues and often significant data providers as well. Unlike the CERTS, which are based on collaborative and hierarchical principles, intergovernmental organizations are composed of equal actors defined by their status as sovereign entities. All of these organizations are driven first and foremost by their own formal mandates and priorities. Thus, to the extent that any large international organization considers security in cyber venues as relevant to their concerns, it is mostly as a secondary priority. However, given the pervasiveness of cyber venues, we expect that these organizations will devote increasing attention to cyber issues in the years to come.

If we focus on organizations that, in principle, have some clear interest or focus on cyberspace, we can identify the major actors and their zones of activity or interest. Unsurprisingly, this leads to a diffuse network of organizations and a wide array of cross-cutting linkages. By way of orientation, we show in Figure 2 several well known international organizations (such as the UN) and new cyber-focused entities that do not have the status of ‘organization’ but are likely to retain a long standing institutional presence on the international arena (such as the World Summit on the Information Society).

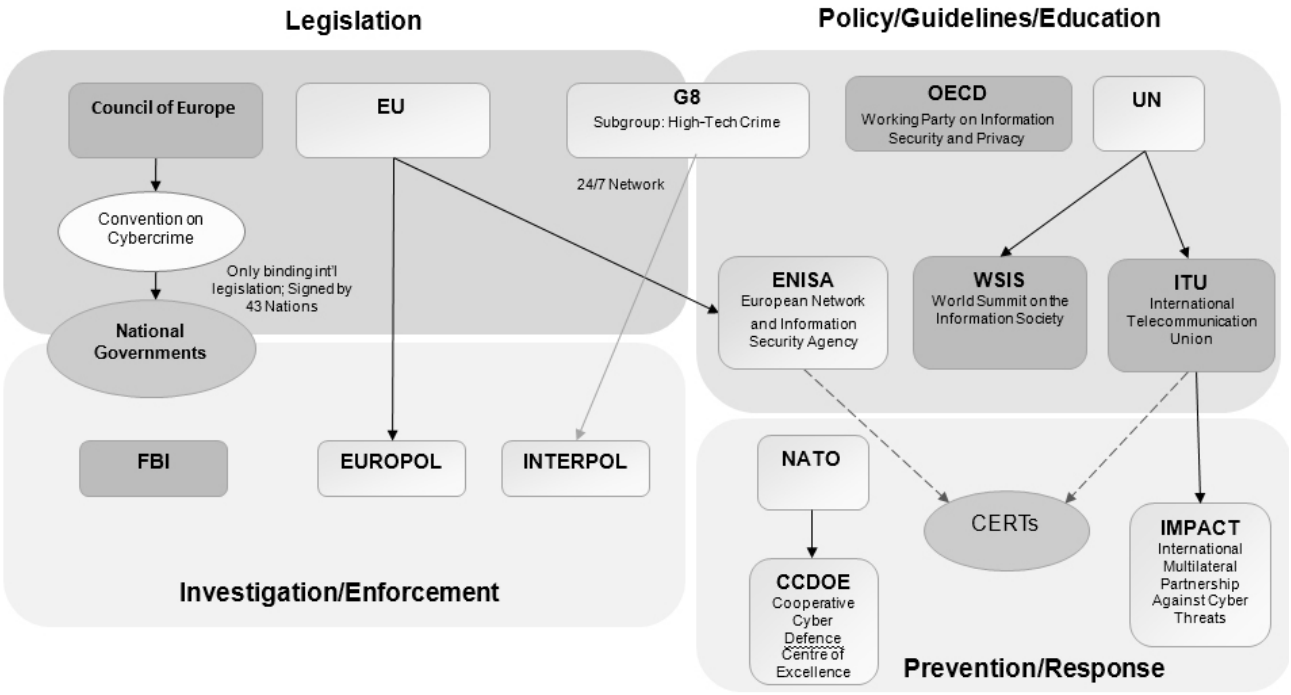


Figure 2. Key Intergovernmental Institutions

Background

The involvement of international organizations in internet security issues can be traced to early meetings of the G8 Subgroup on Hi-Tech Crime. In 1997, the G8, comprised of the world's most developed economies, in cooperation with the International Criminal Police Organization (INTERPOL), established a 24/7 'Network of Contacts' in order to help national governments "identify the source of terrorist communications, investigate threats and prevent future attacks." ("G8 24/7 High Tech Contact Points," 2009). As part of the program, countries were asked to cooperate with INTERPOL in international investigations by sharing information on electronic crimes and by designating an official cybercrime point of contact. While the success rate of the program remains classified, a similar referral model was later mirrored by the FBI in the form of Internet Crime Complaint Center (IC3), which speaks to its relative success. As of 2007, 47 countries were actively involved within the network (Verdelho, 2008).

The 24/7 Network of Contacts is a rare example of direct international intervention. In most cases, international organizations cede direct action to national governments, and instead focus on

organizing conferences that bring together security professionals, academics, law enforcement agencies, and government representatives. These conferences can be seen as part of an evolving process – trial and error – through which international organizations explore the unchartered terrain of cyber security. In addition, the white papers that they publish serve a key role in building international consensus and developing standard practices and guidelines. In many ways this process is an important milestone in the emerging response to cyber threats and the quest for cyber security.

Inter-Governmental Conferences

A closer look at two such conferences, the OECD and the WSIS, helps to clarify the nature of the intergovernmental eco-system by illustrating the broad differences in institutional and statutory status that characterize current inter-governmental initiatives.

OECD-sponsored Conferences.

The OECD has been actively involved in the internet security landscape since 2002 (OECD, 2009a). Meeting twice a year in Paris, the *Working Party on Information Security and Privacy* (WPISP) has published several influential white papers, including "Guidelines for the Security of Information Systems and Networks" (2002), and "Promotion of a Culture of Security for Information Systems and Networks" (2005). These guidelines have been accompanied by stock-taking efforts that track the implementation of policy in member countries (OECD, 2009b). The WPISP has also released several surveys on information security policies in member countries, and has created a 'Culture of Security' Web portal for member states. Since the WPISP is contained within the OECD framework, it represents a formalized extension of OECD's core mission and provides a common approach for all member states.

WSIS.

The World Summit on the Information Society (WSIS) represents the opposite end of the spectrum. Rather than focusing narrowly on security issues, the summit was convened under the auspices of the United Nations as the first comprehensive response to the emergent 'virtual' global society. Interestingly, the WSIS objectives that dealt with cyber security were broadly consistent with the goals and orientation of the WPSIP. Given differences in impetus, legal status, and participation, this alignment of concerns can be seen as another instance of consensus building within the international community.

Operationally, the WSIS was divided into two global conferences. In the first phase, held in Geneva 2003, representatives from over 175 countries committed to a wide-ranging action plan. Action Line C5 focused on "building confidence and security," and committed member countries to increasing security awareness, enacting legislation, and cooperating more extensively with the

private sector (WSIS, 2003). These goals were expanded upon in 2005 at the second phase in Tunis, when member organizations reaffirmed their Geneva commitments and agreed upon a collective stock-taking method to track action line implementation. The efforts by member states to implement Action Line C5 are viewable in a public database, and are also published in annual reports (WSIS, 2009a).

As an UN-based initiative, WSIS decisions were made at the state-level, and only sovereign states served as 'decision-makers.' At the same time, all stakeholders wishing to participate in the overall process – from agenda setting to various forms and forums of deliberations, were encouraged to do so. This inter-governmental response is a milestone in its own right in that it sought to combine several distinct aspects of the UN's 20th development agenda with emergent implications of information technology.

Emerging Responsibilities

For the most part, the foregoing efforts can be seen as 'self-initiated,' whereby private or public entities voluntarily take on a particular function in the emergent cyber security domain. However, more recently the international community has issued operational mandates to specific organizations.

ITU.

The International Telecommunications Union (ITU) was given the primary responsibility for coordinating the implementation of WSIS' Action Plan C5 (WSIS, 2009b). In response, the organization launched the 'Global Cybersecurity Agenda' in 2007. Utilizing a group of high-level experts, ITU provides a variety of resources and toolkits addressing legislation, awareness, self-assessment, botnets, and CERTs (ITU, 2009a). Additionally, ITU publishes guides that educate developing nations on cybercrime and promote best practices and approaches. One of ITU's core missions is to standardize telecommunication technology and release statistics that can be used to track the internet connectivity of nations (ITU, 2009b). Its efforts to promote cyber security arose as a function of the increasing threat rather than as part of its original mission. Thus the international community chose to build upon existing organizational strengths rather than establishing a new institution.

Although the ITU's core competencies are mission specific, they have recently acted in a direct fashion by establishing an arm that will provide international threat response. Envisioned as a global response center focused on combating cyber terrorism and protecting critical infrastructure networks, the *International Multilateral Partnership against Cyber Threats* (IMPACT) is a public-private venture headquartered in Malaysia (UNESCO, 2009). Among other services, IMPACT offers a real-time warning network to 191 member countries, 24/7 response centers, and software that allows security organizations across the globe to pool resources and coordinate their defence

efforts (IMPACT, 2009). Additionally, IMPACT maintains a research division, hosts educational workshops, and conducts high-level security briefings with representatives of member states. These efforts are intended to make IMPACT the "the foremost cyber threat resource centre in the world" (ITU, 2009c).

Although IMPACT has only been operational since March 2009, it is likely that the organization will become a significant provider of technical security data in the near future. If this initiative is successful, then we would have an important precedent for the proposition that an international organization can effectively perform a mission that lies beyond its initial cyber mandate, build upon its core competencies, and extend its regulatory domain in response to technological innovations.

NATO.

In a similar vein to IMPACT, a second major adaptive case is demonstrated by NATO. This intergovernmental organization established a technical response arm in the aftermath of the coordinated attacks on Estonia in 2007. Designated the Cooperative Cyber Defense Centre of Excellence (CCD COE), the entity is responsible for training NATO member states, conducting attack exercises, and supporting NATO in the event of an international cyber attack (Cooperative Cyber Defence Centre of Excellence, 2009). Interestingly, not all NATO states have joined the CCDCOE program, with many countries opting to rely on their own traditional military cyber defense networks. There is no strong evidence that all members of NATO are willing to engage in a common approach to a shared problem, presumably because many states are developing their own strategies for cyber warfare. At the same time, however, the CCDCOE fills an important void for several European states, notably those whose own cyber security capabilities are yet to be developed.

ENISA.

On balance, it is fair to conclude that an overall European technical response has been somewhat limited in scope. Although the European Union has published numerous resolutions on cybercrime, and EUROPOL is actively engaged in investigation, the EU's only substantive action thus far has been the creation of the European Network and Information Security Agency (ENISA). Tasked with a broad mandate "to enhance the capability of the European Union… to prevent, address and respond to network and information security problems," ENISA largely focuses on awareness building, promoting internet safety practices, and working with regional CERTs, and does not provide a comprehensive defense against regional cyber incidents (Europa, 2009).

Convention on Cybercrime.

One area in which European organizations have taken the lead is within the legislative realm. In partnership with the United States, Japan and others, the Council of Europe ratified the *Convention on Cybercrime* in 2004, which remains the only binding international legislation dealing with cybercrime issue (Council of Europe, 2009a). As of September 2009, 26 countries have ratified the treaty, and an additional 20 countries have signed but not yet ratified (Council of Europe, 2009b). The convention defines the criminality of cyber crime, enables law enforcement agencies to effectively investigate electronic crimes, and fosters international cooperation and data sharing (Council of Europe, 2001).

In support of the Convention, the Council of Europe implemented two distinct action plans aimed at training law enforcement agencies and improving national legislation and has hosted global conferences on cybercrime issues annually for the past three years (Council of Europe, 2009c). Additionally, the Council of Europe maintains an extensive database on the progress of national cybercrime legislation (Council of Europe, 2009d). This growth in function is important as it provides evidence of institutionalized response and a broad framework necessary to effectively combat international cyber crime. However, it remains unclear whether the provisions of the Convention will be able to keep pace with the rapid development of the domain; international legislation must necessarily be reactive and will lag behind technological efforts. The true value of the Convention may thus lie in its capacity to 'jump-start' national cyber crime legislation via its provision of an adaptive legal framework.

Data Provision

Although the international security sphere has been growing exponentially over the last half decade, international consensus on cybercrime issues remains in a formative phase. International institutions are focused on building global and local awareness and tend to adopt an advisory or academic role. In this vein, many organizations provide valuable qualitative data, but few provide the quantitative statistics required for robust analysis. As a result, it is difficult to objectively determine the overall performance of these organizations.

This analytical gap may gradually be mitigated as organizations move from a passive posture to an active and fully engaged role within the security landscape, as is evident with the establishment of IMPACT and CCDCOE. Until then, the data provided by inter-governmental organizations can be most effectively used to trace the enactment of legislation, standards, and policies across member states. Utilizing stock taking databases and ratification systems, it should be possible to determine which countries or regions are on the leading edge of enacting the necessary institutional frameworks to properly combat cyber crime.

Finally, it is important to stress that institutionalized data collection activities are always undertaken within a mission-framework. In other words, collection of data is driven by the overall

self-defined objectives and priorities of each organization. This is one of the major sources of non-comparability across data sets. So far, at least, we have not yet seen efforts to standardize definitions, collection procedures, or reporting mechanisms. In one sense, this is not an unexpected development as information standardization usually takes place only after widespread data provision and demand.

IV. National Responses: National Security & Cybercrime

The United States has been at the forefront of institutional response to the new realities formed by cyberspace. It is the leading world power, the state that originally encouraged and supported the creation of cyberspace, and the country that remains renowned for its innovative spirit. By default, the United States has been thrust in a leadership position and has acted as a model for other governmental response to cyber issues, notably in Europe and Asia. But while the United States possesses arguably the strongest known national safeguards against various cyber threats, these programs appear to be far from sufficient. Indeed, according to a recent policy review, "it is doubtful that the United States can protect itself from the growing threat" by maintaining its current security structure (White House, 2009a). The review continues:

> The Federal government is not organized to address this growing problem effectively now or in the future. Responsibilities for cybersecurity are distributed across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions.

In order to trace the foundations of this situation, we must turn to the early federal efforts to combat cyber vulnerabilities. The government initially delegated civilian network defense to the private sector or federally funded organizations such as CERT/CC. In parallel, the intelligence and military communities developed and maintained closeted defense systems. Although the relative technological advantage that these organizations possessed initially allowed them to maintain superiority over external threats, the lack of data sharing and cooperation between agencies, coupled with a rise in global technical competence, led to a growing security dilemma.

After the events of 2001, the United States began a substantial revision of its internet security policy. Through a series of Presidential Directives, the nascent Department of Homeland Security was granted responsibility for cyber internet security efforts. These aims were codified in *The National Strategy to Secure Cyberspace* (2003), which led to a dual approach to cyber defense. With the cooperation of CERT/CC, a national CERT (US-CERT) was established within the National Cyber Security Division of the Department of Homeland Security (DHS) and was tasked with defending federal civil networks (.gov domains). In order to coordinate the actions of various federal agencies, DHS was asked to develop contingency plans and warning systems, and was

granted the ability to coordinate the efforts of 19 federal agencies in the event of a cyber attack of national significance (White House, 2003). Notably, however, the document stressed that "the private sector is best equipped and structured to respond to an evolving cyber threat," and clearly delineated a separate approach for the "national security community" (White House, 2003).

As a result, although the DHS assumed responsibility for a previously neglected area of defense (federal civil networks), the compartmentalization of internet defense strategies continued unchecked. However, it is important to note that this compartmentalization may be a normal byproduct of organizational and bureaucratic politics. As any legal scholar would be quick to point out, this segmentation is not an arbitrary development, rather, it is supported by a legal framework delineated the discrete assignment of responsibilities.

The critical issue here is not that we must move toward a uniform or centralized response to cyber threats. Rather it is that barriers to communication and information sharing --- resulting from legal segmentation --- create added constraints on rapid response to cyber threats. This situation is well appreciated by most if not all parts of the bureaucracy. Although periodic restructuring initiatives have consolidated the security arena, it is recognized that these changes remain marginal given the scale and scope of cyberspace and the associated threat potential. Nevertheless, the government appears committed to discovering valid alternatives, and there are several efforts underway that may result in an effective response structure.

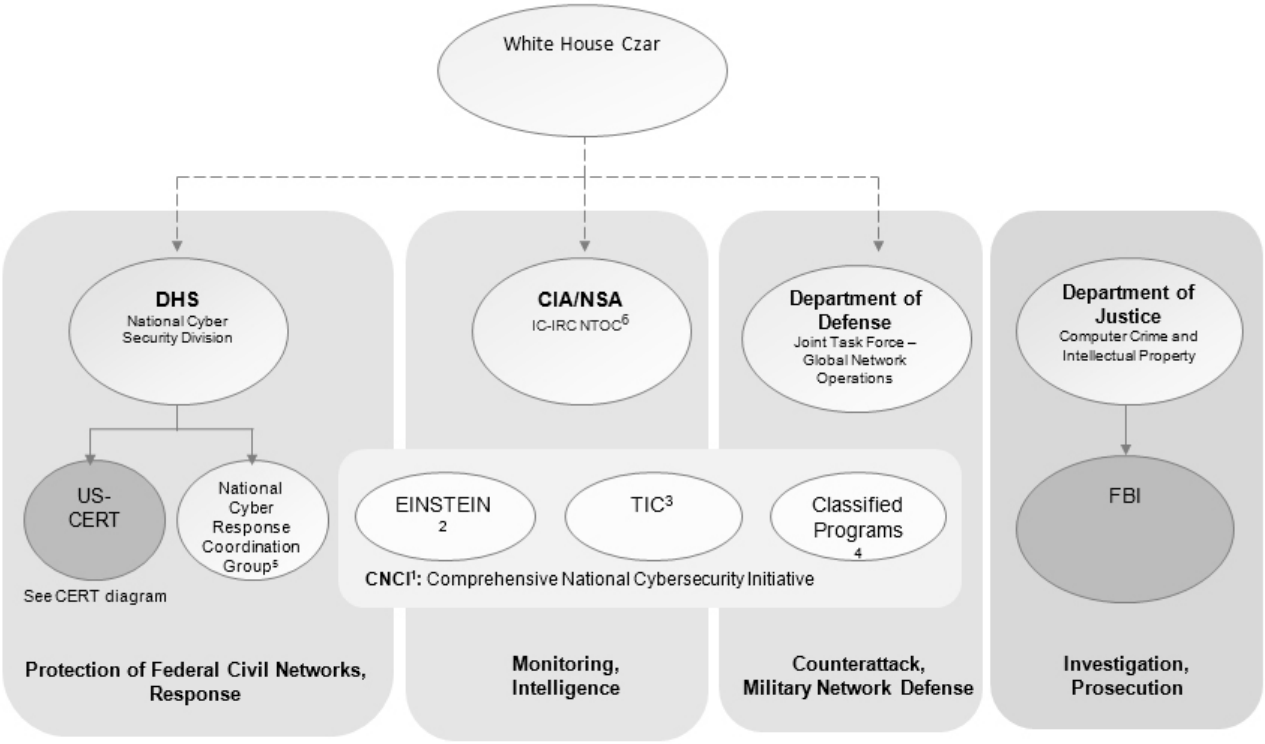
Current Efforts

US cyber policy was further refined in 2008, when President Bush signed a presidential directive establishing the CNCI, or the *Comprehensive National Cybersecurity Initiative*. The initiative reportedly includes several major policy revisions. First, in conjunction with the Office of Management and Budget (OMB), the DHS was tasked with reducing the number of network connections between federal agencies and external providers from 4,000 to 50 within four months (Samson, 2008). Second, an optional DHS program that monitored traffic to and from federal websites, codenamed EINSTEIN, was transferred to the authority of the National Security Agency. The new version of the program will purportedly capture content as well as traffic, and will proactively monitor federal, and possibly private, networks (Samson, 2008). Lastly, the CNCI includes several provisions that are aimed at increasing R&D, coordinating cyber counterintelligence, and promoting information sharing among government organizations (White House, 2009b).

Upon assuming office, President Obama endorsed the CNCI plan, albeit under conditions of increased transparency. Additionally, the White House authorized a sweeping review of cyber policy. Recognizing the increasing compartmentalization of national cyber defense, the final report recommended establishing a cyber security office within the White House. This official (referred to as the Cyber Czar by the press) would be a member of the National Security council, and would

have frequent access to the President.[3] Although the office would not possess the "authority to make policy unilaterally," it would coordinate the responses of federal departments and attempt to bridge communication and policy gaps by "recommend[ing] coherent unified policy guidance… in order to clarify authorities, roles, and responsibilities for cyber security-related activities across the Federal government." Recognizing that "federal responses to cyber incidents have not been unified," the review recommends eliminating overlapping responsibilities between agencies and defining specific roles for cyber defense across government networks (White House, 2009b).

These recommendations are still in the process of being implemented. But considerable strides have been made in providing a coherent logic and rationale for the overall organizational response system. The proposed structure is presented in the Figure 3.



1. **CNCI**: Authorized by President Bush via *Presidential Directive HSPD-23*. CNCI is a classified $17 billion program devoted to improving internet security throughout federal and military networks.
2. **EINSTEIN**: Originally an optional program developed by DHS/US-CERT to monitor federal network intrusion, EINSTEIN is now a classified NSA program devoted to monitoring various internet networks, including the private sector.
3. **Trusted Internet Connections Program**: Devoted to reducing the number of connections to Federal networks from 3000 to 50. Co-sponsored by the OMB.
4. The Department of Defense components of the CNCI program remain classified. It is speculated that they include counteroffensive capability.
5. **NCRG**: The National Cyber Response Coordination Group coordinates the efforts of 19+ Federal agencies in the event of an attack of national significance.
6. **IC-IRC**: Intelligence Community—Incident Response Center, **NTOC**: NSA/CSS Threat Operations Center

Figure 3. Proposed US structure

[3] Note that the position has been established, and is currently filled by Howard Schmidt.

The transition from an organic, overlapping defense network to organized hierarchies is a recurring pattern within the cyber security landscape. However, while centralization and coordination is necessary in order to effectively respond to rapidly evolving threats, inefficient organizational structures may confound the problem by reinforcing barriers to bureaucratic adaptation. While few governments are as large and complex as that of the United States, the fact remains that US cyber policies and the mechanisms for their implementation will provide important signals to other governments,. Even if the US response does not serve as a formal model, its features will be closely scrutinized by others. Concurrently, we must appreciate that the governance of cyberspace is a complex process whose full dimensions are yet to be determined and whose crafting is at an early stage of development

Cyber Crime

An important example of organizational restructuring in the legal domain occurred in 2001, when the FBI collaborated with the National White Collar Crime Center to form the Internet Crime Complaint Center (IC3). Sharing some structural similarities with INTERPOL's 24/7 network, IC3 was created to provide a central contact point for reporting internet crimes. The program is still active today, and by most accounts, has been a success. In 2008 alone, the IC3 processed over 275,000 complaints, 26% of which were deemed valid and referred to law enforcement agencies (National White Collar Crime Center, 2008). However, while the organization serves as a successful model for a national reporting system, this model has been unable to constrain the growth of cyber crime. FBI surveys have shown that most Internet crime remains unreported, and only a fraction of total cyber incidents are processed by the IC3. Furthermore, although the estimated dollar loss of cybercrime has increased every year since 2005, referrals have decreased substantially during the same period (National White Collar Crime Center, 2008).

In some sense, the lack of dramatic success thus far is unsurprising. Efforts to halt the spread of cyber crime suffer from a number of inherent challenges. First, in contrast with traditional crime, the criminality of cyber activities remains ill-defined. Many individuals are not accustomed to reporting cyber crime to law enforcement organizations because issues may be deemed 'minor' or purely technical in nature, or because events on the Internet are deemed outside the jurisdiction of a local police agency. This issue is present in the corporate sphere as well, as many companies view the public acknowledgement of security vulnerabilities as a corporate liability. Second, even when crimes are reported, investigation and prosecution remains difficult. Evidence is often ephemeral and transitory, and the global nature of cyber crime presents serious difficulties in pinpointing the location and identity of criminals. Lastly, it often proves difficult to assess the true monetary damage of cyber crime; for instance, in the case of information theft or security breach. Given that law enforcement agencies possess limited resources, this ambiguity surrounding the true impact of cyber crime creates difficulties in setting investigative priorities.

Although many of the efforts of the FBI and the DOJ have focused on combating cyber crime at the national level, recent initiatives have attempted to ameliorate some of the aforementioned problems by embedding cyber crime experts in local institutions. For instance, since 2003 the FBI has established collaborative Computer Crime Task Forces, which assist police agencies in investigating local cyber crimes. As of 2006, there are over 92 task forces spread throughout the United States (Federal Bureau of Investigation, 2006). In a similar vein, the DOJ has established Computer Hacking & Intellectual Property units in local federal courts, which provide lawyers with the training to effectively understand and prosecute cyber crime.

In recent years, the Federal Trade Commission (FTC) has also played an active role in preventing the spread of cyber crime. This new area of focus was not specifically mandated, but rather arose as a byproduct of efforts to expand the FTC's role in consumer protection. Although the FTC is not tasked with prosecuting or investigating criminal networks, the commission acts by issuing formal complaints and restraining orders against ISPs that are suspected of hosting or promoting illegal activity. These actions prevent ongoing cyber crime activities while prosecution efforts are underway. The FTC thus occupies a critical role in cross-sector collaboration, as the organization possesses the legal authority to rapidly respond to time-sensitive security alerts from NGOs, CERTs, and local government agencies.[4]

In many ways, the United States is simultaneously pursuing centralized and decentralized approaches to combating cyber crime (Figure 3). Critical to the success of either approach is the establishment of a national culture that understands, recognizes, and reports cyber crime. Although statistics on the success of local efforts remain limited, it is important to recognize that initial investments in the sector may not display immediate dividends, due to the necessities of preliminary education and training.

[4] See http://www.internetevolution.com/author.asp?section_id=717&doc_id=177652 for an interesting example of this collaboration.

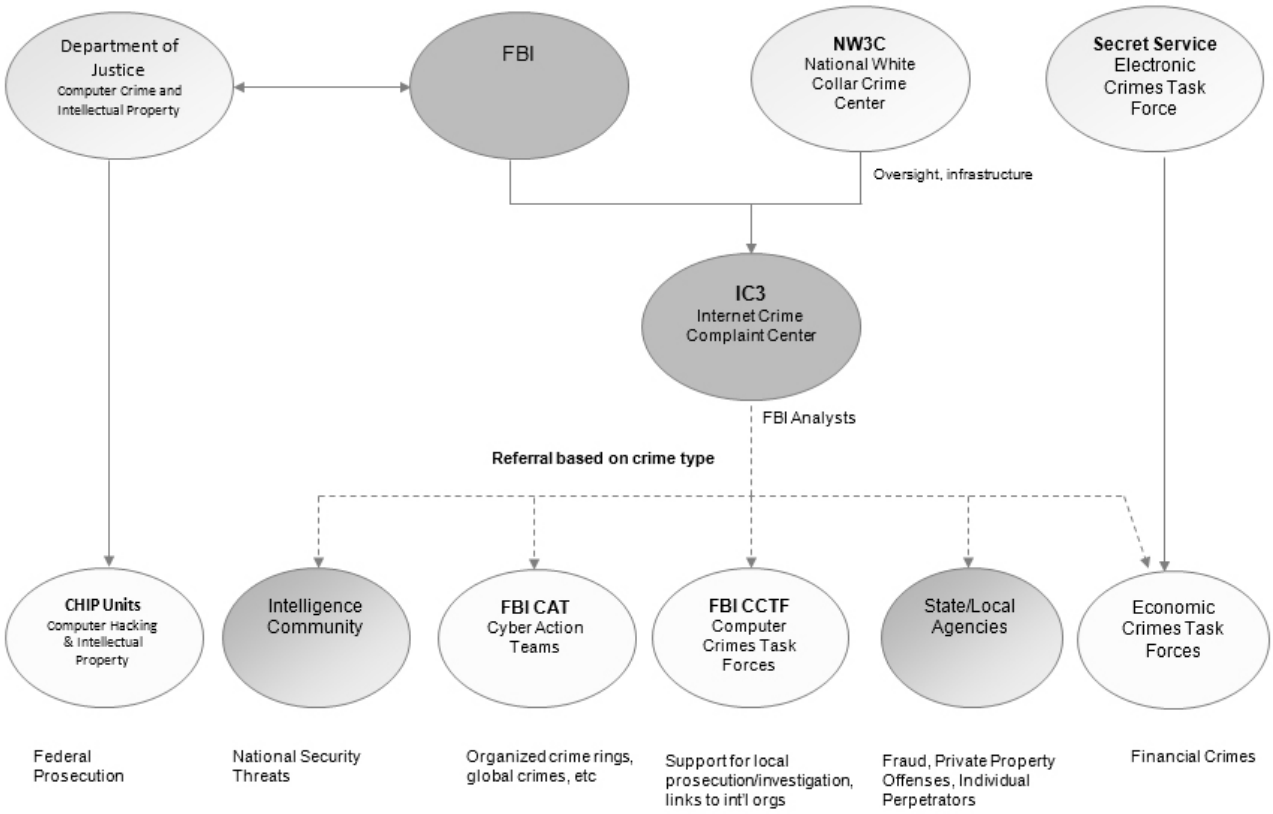


Figure 4. US Investigation/Prosecution Organizations

On Balance

While the process of institutional development is at an early stage, it is possible to chart its course via the use of quantitative data provided by national governments. Although it is unlikely that governments will publically release data related to national security intrusions, data relating to civilian criminal activities is available for a select few countries. For example, in the United States, the Department of Justice maintains a partial database of high-profile cases and convictions, while the FBI regularly publishes IC3 and survey data on cyber crime trends.[5] Similarly, national governments in Korea, Japan, and Taiwan release comprehensive yearly statistics on cyber crime investigations, prosecutions, arrests, and demographic data. Although less directly available, statistics are also provided by countries such as the United Kingdom, Germany, and France.

Unfortunately, however, many nations lack robust legislation dealing with cyber crime; as a result, cyber crime is rarely reported as a distinct category within national police reports. As the

[5] Note, however, that the United States does not currently provide any comprehensive statistics on arrests or prosecutions.

Convention on Cybercrime is ratified by additional countries, it is probable that cybercrime data will become more widely available.

V. End Note

As presented above, the institutional cyber security landscape consists of a complex array of organizations that exhibits significant diversity with regard to missions, mandates, interests, opportunities and constraints. In the best of all possible worlds we would expect to see the emergence of a collaborative framework – a large umbrella network – that allows autonomous organizations to flexibly adapt to emerging threats in a coordinated manner and increases the impetus for information sharing.

Persistent Patterns

While this umbrella network has yet to emerge, we have observed the following organizational responses:

a) Not-for-Profit institutions designed to focus on cyber threats (CERT/CC, FIRST, and private CERTs). In some instances, these institutions have transitioned to private-public partnerships.
b) International institutions established to manage interactions among advanced states (OECD).
c) International conferences designed to communicate the potential for information technology to facilitate transitions towards sustainable development (WSIS).
d) Functional international organizations with core missions and competencies (ITU).
e) National agencies tasked with responding to cyber crime (FBI).
f) Development of binding international legislation (Convention on Cybercrime).
g) Organizations and strategies focused on the defense of military and intelligence networks (CCDOE, CNCI).

Each of these institutional responses has different mandates, rules and responsibilities. None are accorded complete regulatory power. Indeed, there is little evidence of overarching institutional coordination or routinization. On one hand, this pattern represents a certain degree of disconnect. On the other, it can be seen as a dynamic and shifting response to an emerging threat. In the latter context, one could argue that the increasingly dense landscape of institutional responses is an excellent indication that the international community is taking serious steps to control a cyber threat of epidemic proportions.

Potential Trends

On these bases we put forth the following propositions:

a) The current institutional landscape resembles a security patchwork that covers critical areas rather than an umbrella that spans all of the known modes and sources of cyber threat.
b) Given the multiple contexts and diverse institutional motivations, we expect that responses will be driven more by institutional imperatives and reactions to crisis than by coordinated assessment and proactive response.
c) Due to the complex global agenda at all levels of development, states may not be willing to proceed until international norms are developed, rather they will 'take matters in their own hands' and develop first order responses.
d) Cross-sector collaboration between public, private, and volunteer organizations may serve as a temporary measure to cover holes in the current defense network. However, at some point effective institutions will be necessary; they may develop in parallel with rising public awareness.

As of this writing we have not yet seen large terrorist groups engaged in cyber malfeasance. This pattern cannot be expected to continue. Recent efforts to infiltrate critical US infrastructure and the devastating attacks on Estonia and Georgia in 2007 and 2008 underline the dangers of being lulled into a false sense of security. As the Internet becomes increasingly central to modern society, it is likely that criminals, terrorist groups, and other opponents to state authority will target the sector in the hopes of disrupting critical national functions. So far the potential for significant threats is far greater than institutional capabilities to contain these threats. In other words, the 'demand' for security far exceeds the provision of effective 'supply.'

Data Analysis

Although the current system of institutional arrangements shows signs of weakness, it is also true that the level of organization and cooperation has been steadily increasing. To some degree, the effectiveness of this effort can be quantified through the use of statistics. While a relatively small number of organizations produce reliable data, sufficient information exists to develop a model that maps the degree of vulnerability versus the effectiveness of organizational response. For instance, international data on cyber crime legislation and awareness can be correlated with arrest rates in individual countries. When combined with stocktaking databases, this method allows one to determine the rate of progress in individual nations versus cybercrime issues. Similarly, quantitative data provided by national CERTs can be used to obtain insights about their performance in their respective national contexts and constituencies. An example of these kinds of analysis, along with a

Data Dashboard tool, can be found in the report “Experiences and Challenges with using CERT Data to Analyze International Cyber Security” (Madnick et al, 2009).

Over time, we anticipate the possibility of pairing international and national statistics with information from the private sector. Security and monitoring companies such as Symantec, Arbor Networks, Microsoft, and McAfee provide quantitative data that address the global spread of internet vulnerabilities. In many cases, the volume and quality of data released by these organizations far outpaces the information released by international and national organizations. However, the true value of this information lies not in an isolated analysis, but in the intersection of private data with the national and international sphere. For instance, statistics concerning the originating country of cyber attacks or the absolute volume of attacks can potentially be paired with national CERT data to determine the degree of national vulnerabilities and traffic that each CERT is capable of handling.

These metrics, and others that can potentially be derived, may provide a powerful method of simultaneously evaluating data quality and organizational performance. An important next step in our inquiry is to examine additional data providers and explore ways of pairing this data with national and international organizations to form evaluative statistical models. While doing so, it is important to remain cognizant of the institutional context that that enables or constrains the provision of information.

Acknowledgement

This work was funded, in part, by the Office of Naval Research. Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the Office of Naval Research.

References

CERT Program. (2009a). *About CERT*. Retrieved on September 17, 2009, from http://www.cert.org/meet_cert/

CERT Program. (2009b). *CERT statistics (historical).* Retrieved on September 26, 2009, from http://www.cert.org/stats/cert_stats.html

Cooperative Cyber Defence Centre of Excellence. Retrieved on January 11, 2009, from http://www.ccdcoe.org/11.html

Council of Europe. (2001). *ETS No. 185 - Convention on cybercrime*. Retrieved on September 19, 2009, from http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Council of Europe. (2009a). *Council of Europe action against economic crime.* Retrieved on September 28, 2009, from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Default_en.asp

Council of Europe. (2009b). *Convention on cybercrime*. Retrieved on September 27, 2009, from http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=09/09/2009&CL=ENG

Council of Europe. (2009c). *Project on cybercrime (phase 1).* Retrieved on September 26, 2009, from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime%5Ccy%20Project/projectcyber_en.asp

Council of Europe. (2009d). *Cybercrime legislation - country profile*s. Retrieved on September 28, 2009, from http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp

Federal Bureau of Investigation. (2006). *Netting cyber criminals*. Retrieved on February 20, 2010, from http://www.fbi.gov/page2/jan06/ccctf012506.htm

Forum of Incident Response and Security Teams. (2009a). *Alphabetical list of FIRST members.* Retrieved on September 20, 2009, from http://www.first.org/members/teams/

Forum of Incident Response and Security Teams. (2009b). *FIRST history*. Retrieved on September 29, 2009, from http://www.first.org/about/history/

Europa. *European Network and Information Security Agency (ENISA).* Retrieved on September 21, 2009, from http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l24153_en.htm

G8 24/7 High Tech Contact Points. *Cyber Security Co-Operation.* Retrieved on October 28, 2009, from http://www.cybersecuritycooperation.org/moredocuments/24%20Hour%20Network/24%207%20invitation.pdf

IMPACT. *Welcome to the coalition.* Retrieved on October 23, 2009, from http://www.impact-alliance.org/

International Telecommunication Union. (2009a). *Global Cybersecurity Agenda (GCA).* Retrieved on September 25, 2009, from http://www.itu.int/osg/csd/cybersecurity/gca/

International Telecommunication Union. (2009b). *Information and communication technology (ICT) statistics*. Retrieved on September 25, 2009, from http://www.itu.int/ITU-D/ict/

International Telecommunication Union. (2009c). *Global Cybersecurity Agenda (GCA): Technical and security measures*. Retrieved on September 25, 2009, from http://www.itu.int/osg/csd/cybersecurity/gca/tech-proced.html

Killcrece, Georgia. (2004). *Steps for creating national CERTs*. Carnegie Mellon Software Engineering Institute. Retrieved on September 13, 2009, from http://www.cert.org/archive/pdf/NationalCSIRTs.pdf

Krebs, Bryan. (2008, May 15). Government secrecy and the mysterious cyber initiative. *The Washington Post*. Retrieved on September 25, 2009, from http://voices.washingtonpost.com/securityfix/2008/05/government_secrecy_and_the_mys.html

Madnick, Stuart, Li Xitong, & Choucri, Nazli. (2009). *Experiences and challenges with using CERT data to analyze international cyber security*. Proceedings of the AIS SIGSEC Workshop on Information Security & Privacy (WISP 2009), Phoenix, Arizona, December 2009, pp. 6-16.

Nakashima, Ellen (2008, January 26). Bush order expands network monitoring. *The Washington Post*. Retrieved on September 26, 2009, from http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html

National White Collar Crime Center. (2008). *IC3 annual report*. Retrieved on September 23, 2009, from http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf

Samson, Victoria. (2008, July 23). The murky waters of the White House's cybersecurity plan. *Center for Defense Information*. Retrieved on September 26, 2009, from http://www.cdi.org/program/document.cfm?DocumentID=4345&from_page=../index.cfm

OECD. (2009a). *What is the Working Party on Information Security and Privacy (WPISP)?* Retrieved on October 23, 2009, from http://www.oecd.org/document/46/0,3343,en_2649_34255_36862382_1_1_1_1,00.html

OECD. (2009b). *Initiatives by country.* Retrieved on September 27, 2009, from http://www.oecd.org/document/63/0,3343,en_21571361_36139259_36306559_1_1_1_1,00.html

UNESCO. (2009, March 23). *UN-backed anti-cyber-threat coalition launches headquarters in Malaysia*. Retrieved on March 24, 2009, from http://portal.unesco.org/ci/en/ev.php-URL_ID=28464&URL_DO=DO_TOPIC&URL_SECTION=201.html

Verdelho, Pedro. (2008). *The effectiveness of international co-operation against cybercrime*. Council of Europe. Retrieved on September 27, 2009, from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/DOC-567study4-Version7_en.PDF/

The White House. (2003). *The National Strategy to Secure Cyberspace*. Retrieved on September 20, 2009, from http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

The White House. (2009a). *Cyberspace policy review: assuring a trusted and resilient information and communications infrastructure.* Retrieved on September 23, 2009, from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

The White House. (2009b). *The Comprehensive National Cybersecurity Initiative.* Retrieved on March 20, 2010, from http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

WSIS. (2009a). *Stocktaking*. Retrieved on October 17, 2009, from http://www.itu.int/wsis/stocktaking/index.html

WSIS. (2009b). *WSIS C5*. Retrieved on October 17, 2009, from http://www.itu.int/osg/csd/cybersecurity/WSIS/

WSIS. (2003). *Plan of action.* Retrieved on October 17, 2009, from http://www.itu.int/wsis/docs/geneva/official/poa.html